UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,140	02/01/2002	Satyendra Yadav	10559-755001	5189

20985 7590 11/15/2005

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,140	YADAV, SATYENDRA	
	Examiner	Art Unit	
	Venkatanarayanan Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *13-21 and 26-33* is/are allowed.

6)☐ Claim(s) *1-10 and 22-25* is/are rejected.

7)☐ Claim(s) *11 and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. The Applicant's arguments regarding Claim 1, 22, and 24 are not persuasive. As Markham(U.S. Patent Publication 2003/0126468 A1) discloses the application-specific network policies see Par. 0076(when Telneting the policies are adapted to block both incoming and outgoing) and the authorization of application see Par. 0094 & Par. 0098.

2. The Applicant's arguments regarding Claim 13, 26, 31 are persuasive. As Markham discloses the detection of abnormal behavior see Par. 0084, which is an parameter included in the application specific signature as disclosed in the Specifications see Page 23 Par. 0066. However, the signatures related to applications being loaded form a central security server as disclosed in the Specifications see Par.044 is absent in the prior art. And further arguments with regard to Claim 31 is persuasive, the absence of fabricated response in Markham.

3. The Applicant's arguments regarding Claim 2 and 3 is not persuasive. As the authorizing of inbound communication, blocking(filtering) and monitoring to detect intrusion from a particular source see Par.0094-0100.

4. The Applicant's argument regarding Claim 9 and 10 are not persuasive. As Markham discloses the monitoring of application and identifying the application see Par. 0100.

5. The Applicant's arguments regarding Claim 11 and 12 are persuasive. As Markham is silent with respect to applying hash function to invoked application's executable and the running of detection system and application in a single execution context.

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

Claim Rejections - 35 USC § 102

7. Claim 1-10, 22-25 are rejected under 35 U.S.C. 102(e) as being U.S. Patent Publication 2003/0126468 B1 by Markham with priority under 35 U.S.C § 119(a) based on PCT No. PCT/US01/17153.

8. Regarding Claim 1, Markham discloses the receiving requests for network communications services, selectively designating each of received requests as authorized or unauthorized, monitoring inbound communications, based on authorized requests to detect intrusion see Par. 0011-0012 & Par. 0029 & Par. 0094.

9. Regarding Claim 2, Markham discloses the blocking of inbound network communications and monitoring the blocked inbound network communications see Par. 0036.

10. Regarding Claim 3, Markham discloses the examining blocked inbound communications, identifying the source and initiating monitoring of inbound communication from that source see Par. 0032 & Par. 0034.

11. Regarding Claim 4, Markham discloses the examining the blocked network communications by checking for patterns see Par. 0015 & par. 0083-0087.

12. Regarding Claim 5, Markham discloses the responses to monitoring blocked inbound communication see Par. 0100.

13. Regarding Claim 6, Markham discloses the checking inbound communications identified from the packet-level exploits see Par. 0034.

14. Regarding Claim 7, Markham discloses the updating the packet filter in response to unauthorized requests see Par. 0014-0015.

15. Regarding Claim 8, Markham discloses the monitoring of network communications initiated by application specific intrusion signature see Par. 0094-0096.

16. Regarding Claim 9, Markham discloses the examining the set of instructions of the application see Par. 0100.

17. Regarding Claim 10, Markham discloses the invoking the intrusion detection by invoked application and being executed within a single context see Par. 0104-0106.

18. Regarding Claim 22, Markham discloses the network requests that fail to satisfy the application-specific network policy and also by mutual exclusion the requests that satisfy the network policy see Par. 0083; the blocking of network communications that do not satisfy the application-specific network policy see Par. 0074-0076; the responding to blocked network communications see Par. 0078 & Par. 0100.

19. Regarding Claim 23, Markham discloses "network policy enforcer" and "network traffic enforcer" being shared in part of intrusion detection system see Par. 0096 & Par. 0091.

20. Regarding Claim 24, Markham discloses the receiving requests for network communications services, selectively designating each of received requests as authorized or unauthorized, monitoring inbound communications, based on authorized requests to detect intrusion see Par. 0011-0012 & Par. 0029 & Par. 0094, detection in response to intrusion prelude and identified abnormal application behavior see Par. 0083-0084 & Par.0100.

21. Regarding Claim 25, Markham discloses the responding to attacks and further redirect the packets for further analysis see Par. 0087 & Par. 0015.

Allowable Subject Matter

22. Claims 13-21, 26-27, and 31-33 are allowed. The following is a statement of reasons for the indication of allowable subject matter: The Applicant's arguments regarding Claim 11-13, 26, 31 are persuasive, see the discussion above in *Response to Arguments.*

23. Claims 11 and 12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

VP
11/9/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100